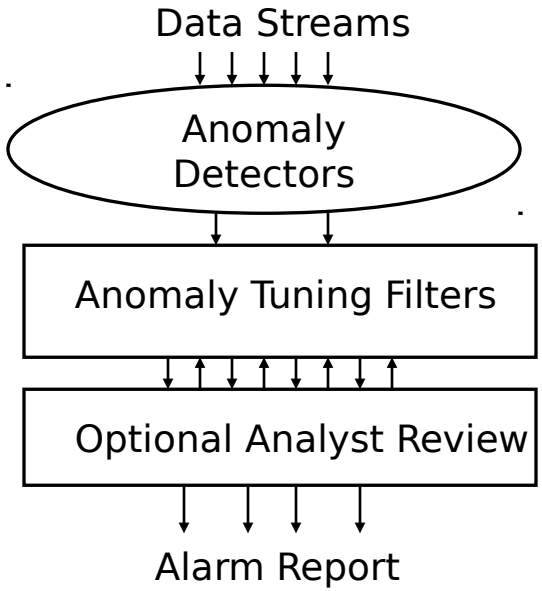
Architecture



New Ideas

- Detecting unanticipated anomalies.
- Calibrated benchmark data sets.
- Selecting critical variables from high-dimensional data sets using local, not global, estimates of dimensionality.
- Visual confirmation of anomaly alarms.
- Synthesizing datasets for sensitivity tests.
- Making a synthetic environment available as a World Wide Web service.

Carnegie Mellon

Impact

- Will be usable for detecting unusual or intrusive behavior in security-critical arenas, as well as in a wide variety of process and mission-critical systems.
- Will improve detector accuracy through use of benchmark data sets.
- Will dramatically reduce system downtime due to early warnings provided by anomaly trending & event prediction.

Schedule

Year 1: - Designing & prototyping
- Synthesizing data

Year 2: - Hardening prototypes
- Acquiring industrial partner/data
- Benchmarking
- Piloting WWW site

Year 3: - Operating on industrial data
- Evaluating effectiveness
- Unrestricted access WWW site